Self-embeddings of cyclic and projective Steiner quasigroups

Diane M. Donovan[1*], Mike J. Grannell[2], Terry S. Griggs[2],
James G. Lefevre[1*] and Thomas McCourt[1]
1. Centre for Discrete Mathematics and Computing
University of Queensland
St Lucia 4072, Australia
2. Department of Mathematics and Statistics
The Open University
Walton Hall
Milton Keynes MK7 6AA, UK

Abstract

It is shown that for every admissible order v for which a cyclic Steiner triple system exists, there exists a biembedding of a cyclic Steiner quasigroup of order v with a copy of itself. Furthermore, it is shown that for each $n \geq 2$ the projective Steiner quasigroup of order $2^n - 1$ has a biembedding with a copy of itself.

AMS Subject Classifications: primary 05B15; secondary 05B07, 05C10.

Keywords: Complete tripartite graph, Embedding, Latin square, Steiner quasigroup, Steiner triple system.

---

[*] Donovan and Lefevre supported by grants DP0664030 and LX0453416

1 Introduction

This paper is mainly concerned with triangular embeddings of complete regular tripartite graphs $K_{n,n,n}$ in orientable surfaces. For background material on graph embeddings, the reader is referred to the books by Gross and Tucker [13] and by Ringel [16]. As noted in [8], a triangular embedding of $K_{n,n,n}$ is face 2-colourable if and only if the supporting surface is orientable. In such a case, the faces in each colour class can be regarded as the triples of a transversal design with block size three, or equivalently as a Latin square with rows, columns and entries identified as the three vertex sets of the graph partition. The two Latin squares are said to be *biembedded* in the surface. A biembedding of two paratopic Latin squares (that is, two squares in the same main class) is referred to as a *self-embedding*. This leads naturally to the question of which main classes of Latin squares admit biembeddings, either with paratopic copies of themselves, or with Latin squares from different main classes.

To date, attention has focused on Latin squares which are the Cayley tables of Abelian groups. The unique *regular* triangular embedding of $K_{n,n,n}$, so called because it exhibits the greatest possible degree of symmetry, was constructed by Stahl and White [17] using a voltage graph based on a dipole with n parallel edges embedded in a sphere. The Latin squares biembedded are the Cayley table of the cyclic group $\mathbb{C}_n$ with a paratopic copy of itself. An alternative approach to this biembedding, constructed directly from the Latin squares themselves is given in [6]. Further biembeddings of the Cayley table of a cyclic group both with a paratopic copy of itself and with Latin squares in other main classes are given in [3] and [4]. In [9] and [11], it is proved that there exists a biembedding of the Cayley table of every Abelian group with the single exception of the group $\mathbb{C}_2 \times \mathbb{C}_2$.

In this paper we will be concerned with Latin squares which are the composition tables of cyclic Steiner quasigroups. In particular, we prove that for all admissible orders for which a cyclic Steiner quasigroup exists, there exists a biembedding of the composition table of a cyclic Steiner quasigroup of that order with a paratopic copy of itself. We go on to show that for each $n \geq 2$ the projective Steiner quasigroup of order $2^n - 1$ has a biembedding with a copy of itself. Finally, we note that these self-embeddings of projective Steiner quasigroups facilitate improved lower bounds for the numbers of nonisomorphic triangular embeddings of complete regular tripartite graphs and of complete graphs of certain orders. We begin with some basic definitions.

Recall that a Steiner triple system of order v, $S = \mathrm{STS}(v)$, is an ordered pair $(V, \mathcal{B})$ where V is a set of cardinality v and $\mathcal{B}$ is a collection of *triples*, also called *blocks*, which has the property that each pair of distinct elements of V occurs in precisely one triple. The necessary and sufficient condition for the existence of an $\mathrm{STS}(v)$ is that $v \equiv 1$ or $3 \pmod 6$ [14]; such values are said to be *admissible*. Given an $\mathrm{STS}(v)$, an algebraic structure, called a *Steiner quasigroup* or *squag*, on V can be constructed with the operation $\circ$ defined by $x \circ x = x$ for all $x \in V$, and $x \circ y = z$ for all $x, y \in V$ with $x \neq y$, where $\{x, y, z\} \in \mathcal{B}$.

In this paper we will be concerned with *cyclic* Steiner triple systems. These are $\mathrm{STS}(v)$ which have an automorphism of order v. The standard representation is on the set $V = \mathbb{Z}_v = \{0, 1, 2, \ldots, v-1\}$ with the automorphism generated by the mapping $i \mapsto i + 1 \pmod v$. We assume this representation throughout, including in the statements and proofs of the theorems. It was shown in [15] that cyclic $\mathrm{STS}(v)$ exist for all admissible values of v except for $v = 9$. A cyclic $\mathrm{STS}(v)$ gives rise to a Steiner quasigroup which is itself cyclic in the sense that $x \circ y = z$ if and only if $(x+1) \circ (y+1) = z+1$.

Cyclic Steiner triple systems are closely related to solutions of Heffter's difference problems, [5, 2]. Heffter's first difference problem, $\mathrm{HDP}_1(m)$, is to find a partition of the integers $\{1, 2, \ldots, 3m\}$ into m triples (a_i, b_i, c_i), $i = 1, 2, \ldots, m$, such that either $a_i + b_i = c_i$ or $a_i + b_i + c_i \equiv 0 \pmod{6m+1}$. Given a solution to $\mathrm{HDP}_1(m)$, a cyclic $\mathrm{STS}(6m+1)$ can be constructed by choosing as orbit starters, for each $i : 1 \leq i \leq m$, either the triple $\{0, a_i, a_i + b_i\}$ or the triple $\{0, b_i, a_i + b_i\}$. Hence, every solution to $\mathrm{HDP}_1(m)$ generates 2^m different, but possibly isomorphic, cyclic $\mathrm{STS}(6m+1)$. Heffter's second difference problem, $\mathrm{HDP}_2(m)$, $m \geq 2$, is similar; to partition the integers $\{1, 2, \ldots, 3m+1\} \setminus \{2m+1\}$ into triples as above (working modulo $6m+3$). With the additional short orbit generated by the triple $\{0, 2m+1, 4m+2\}$, every solution to $\mathrm{HDP}_2(m)$ generates 2^m different cyclic $\mathrm{STS}(6m+3)$. The converse of these implications also holds true; given a cyclic $\mathrm{STS}(v)$, a solution of the corresponding Heffter difference problem may be obtained from orbit starters of the form $\{0, \alpha, \beta\}$.

We represent embeddings by means of *rotation schemes*. Suppose that L and L' are two Latin squares of order v, defined on the same row set $\{0_r, 1_r, \ldots, (v-1)_r\}$, the same column set $\{0_c, 1_c, \ldots, (v-1)_c\}$, and the same entry set $\{0_e, 1_e, \ldots, (v-1)_e\}$. The *rotation* about a point x_r is defined to be the set of cycles

$$(y_c^0 z_e^0 y_c^1 z_e^1 \dots y_c^{a_1-1} z_e^{a_1-1})(y_c^{a_1} z_e^{a_1} \dots y_c^{a_2-1} z_e^{a_2-1}) \dots (y_c^{a_{n-1}} z_e^{a_{n-1}} \dots y_c^{v-1} z_e^{v-1})$$

where $z^i = L(x, y^i)$, $i \in \{0, 1, \dots, v-1\}$, and $z^i = L'(x, y^{i+1})$, $i \in \{0, 1, \dots, v-1\} \setminus \{a_1 - 1, a_2 - 1, \dots, a_n - 1\}$ where $a_n = v$, and $z^{a_j - 1} = L'(x, y^{a_{j-1}})$, $1 \leq j \leq n$ where $a_0 = 0$. The rotation about a point y_c is defined analogously, alternating entry points and row points obtained from column y of L and L'. Similarly, the rotation about a point z_e alternates row points and column points obtained from entries z in L and L'. The two Latin squares L and L' are biembedded in a surface (rather than a pseudosurface) if and only if the rotation about each point is a single cycle, and in such a case we write $L \bowtie L'$. The entire set of rotations is then called the rotation scheme for the biembedding of L and L', and we also use the notation $L \bowtie L'$ to denote this biembedding.

2 Self-embeddings of cyclic Steiner quasigroups.

Theorem 2.1 *Let S and T be cyclic STS$(6m+1)$ with orbit starters $\{0, a_i, a_i + b_i\}$ and $\{0, b_i, a_i + b_i\}$ respectively, $1 \leq i \leq m$, obtained from a solution to HDP$_1(m)$. Further, let L_S and L_T be the Latin squares of the composition tables of the Steiner quasigroups obtained from S and T. Let L_T^d be the Latin square obtained by adding d (mod $6m+1$) to every entry of the square L_T. If the rotation in L_S and L_T^d about the point 0_r is a single cycle, then $L_S \bowtie L_T^d$.*

Proof. The rotation about the point 0_r is a single cycle, say

$$(x_c^0 y_e^0 x_c^1 y_e^1 \dots x_c^{v-1} y_e^{v-1}).$$

First consider rotations about points k_r, $1 \leq k \leq v-1$. Since both S and T are cyclic, the rotation about the point k_r is

$$((x^0 + k)_c (y^0 + k)_e (x^1 + k)_c (y^1 + k)_e \dots (x^{v-1} + k)_c (y^{v-1} + k)_e),$$

also a single cycle.

Now consider rotations about points k_c, $0 \leq k \leq v-1$. Since both Latin squares L_S and L_T^d are symmetric, the permutation

$$((x^0 + k)_r (y^0 + k)_e (x^1 + k)_r (y^1 + k)_e \dots (x^{v-1} + k)_r (y^{v-1} + k)_e)$$

is also a single cycle. The reverse of this cycle gives the rotation about the point k_c, oriented consistently with the rotations about the points k_r.

Next consider the rotation about the point 0_e. Define permutations

$$P_1 = \prod_{1 \le i \le m} (a_i\ \ (a_i + b_i))(-a_i\ \ b_i)((-a_i - b_i)\ \ \ -b_i),$$

$$P_2 = \prod_{1 \le i \le m} (a_i\ \ \ -b_i)((a_i + b_i)\ \ b_i)(-a_i\ \ (-a_i - b_i)).$$

Further let R^d be the permutation determined by the mapping $i \mapsto i + d \pmod{v}$, $0 \le i \le v - 1$.

Then the permutation $(x^0\ x^1\ \ldots\ x^{v-1})$ obtained from the column entries of the rotation about the point 0_r satisfies

$$(x^0\ x^1\ \ldots\ x^{v-1}) = P_2 R^{-d} P_1.$$

(Here and subsequently in a composition AB of permutations A and B, it is understood that B is applied first.) Similarly the permutation obtained from the row entries of the rotation about the point 0_e is $R^{-d}P_2R^dP_1$. We need to prove that this is a single cycle.

First observe that

$$P_2P_1P_2 = P_1P_2P_1 = \prod_{1 \le j \le 3m} (-j\ \ j)$$

and hence that $P_2P_1P_2R^d = R^{-d}P_1P_2P_1$. Therefore

$$P_2R^dP_1 = P_1^{-1}P_2^{-1}R^{-d}P_1P_2P_1P_1 = P_1P_2R^{-d}P_1P_2$$

since both P_1 and P_2 are involutions. So $R^{-d}P_2R^dP_1 = R^{-d}P_1P_2R^{-d}P_1P_2 = R^{-d}P_1P_2R^{-d}P_1P_2R^{-d}P_1P_1R^d = R^{-d}P_1(P_2R^{-d}P_1)^2(R^{-d}P_1)^{-1}$; that is, $R^{-d}P_2R^dP_1$ is conjugate to $(P_2R^{-d}P_1)^2$. But $P_2R^{-d}P_1$ is a single cycle and hence, since v is odd, so is $(P_2R^{-d}P_1)^2$.

Finally consider rotations about points k_e, $1 \le k \le v - 1$. Again, since both S and T are cyclic, the rotation about the point k_e is obtained by adding k to each point of the rotation about the point 0_e. □

The above theorem can be readily extended to cyclic STS$(6m + 3)$s with orbit starters obtained in the same way from a solution to HDP$_2(m)$, together with the short orbit generated by the triple $\{0, 2m + 1, 4m + 2\}$. The proof is the same as that of the previous theorem with the permutations P_1 and P_2 amended to

$$P_1 = \prod_{1\le i\le m} (a_i \ \ (a_i+b_i))(-a_i \ \ b_i)((-a_i-b_i) \ \ -b_i)((2m+1) \ \ (4m+2)),$$

$$P_2 = \prod_{1\le i\le m} (a_i \ \ -b_i)((a_i+b_i) \ \ b_i)(-a_i \ \ (-a_i-b_i))((2m+1) \ \ (4m+2)).$$

Thus we have the following theorem:

Theorem 2.2 *Let S and T be cyclic $STS(6m+3)$ with orbit starters $\{0, a_i, a_i+b_i\}$ and $\{0, b_i, a_i+b_i\}$ respectively, $1 \le i \le m$, obtained from a solution to HDP$_2(m)$, together with the short orbit generated by the triple $\{0, 2m+1, 4m+2\}$. Further, let L_S and L_T be the Latin squares of the composition tables of the Steiner quasigroups obtained from S and T. Let L_T^d be the Latin square obtained by adding d (mod $6m+3$) to every entry of the square L_T. If the rotation in L_S and L_T^d about the point 0_r is a single cycle, then $L_S \bowtie L_T^d$.*

Theorems 2.1 and 2.2 give a sufficient condition for establishing that $L_S \bowtie L_T^d$. Since the condition is obviously necessary, these theorems provide a simple test to determine whether or not the Latin squares L_S and L_T^d can be biembedded in a surface. Note that the Steiner systems S and T are isomorphic, the mapping $i \mapsto v-i$ carrying the isomorphism. Thus the Latin squares L_S and L_T which are the composition tables of the Steiner quasigroups obtained from S and T respectively are in the same main class, as is the Latin square L_T^d. So, whenever the test is satisfied, there exists a self-embedding of the Latin square of the composition table of the corresponding Steiner quasigroup. We illustrate this with examples for $v = 7, 13$ and 15; as noted in the Introduction, there is no cyclic STS(9).

Example 2.1 The unique STS(7) is cyclic and can be obtained from the solution $(1, 2, 3)$ of HDP$_1(1)$. Let S be generated by the orbit starter $\{0, 1, 3\}$ and T by the orbit starter $\{0, 2, 3\}$. If we take $d = 1$, the rotation about 0_r is

$$(0_c 0_e 4_c 5_e 6_c 2_e 5_c 4_e 2_c 6_e 1_c 3_e 3_c 1_e).$$

Thus $L_S \bowtie L_T^1$.

Example 2.2 There is a unique cyclic STS(13) obtained from the solution $(1,3,4),(2,5,6)$ of $\mathrm{HDP}_1(2)$. Let S be generated by the orbit starters $\{0,1,4\}$, $\{0,2,7\}$ and T by the orbit starters $\{0,3,4\}$, $\{0,5,7\}$. Again take $d=1$. The rotation about 0_r is

$$(0_c 0_e 9_c 10_e 12_c 3_e 8_c 6_e 7_c 2_e 10_c 9_e 2_c 7_e 11_c 5_e 3_c 12_e 6_c 8_e 5_c 11_e 1_c 4_e 4_c 1_e).$$

Again $L_S \bowtie L_T^1$.

Example 2.3 There are two cyclic STS(15)s. Both can be obtained from the solution $(1,3,4)$, $(2,6,7)$ of $\mathrm{HDP}_2(2)$. One cyclic system, which is the point-line design of the projective geometry PG$(3,2)$, can be constructed by taking the orbit starters $\{0,1,4\}$, $\{0,2,8\}$, $\{0,5,10\}$; let this be system S. Then system T has orbit starters $\{0,3,4\}$, $\{0,6,8\}$, $\{0,5,10\}$. Taking $d=1$ again gives a biembedding of L_S and L_T^1.

The other cyclic STS(15), which is the unique anti-Pasch STS(15), can be constructed by taking the orbit starters $\{0,1,4\}$, $\{0,6,8\}$, $\{0,5,10\}$; let this be system S. Then system T has orbit starters $\{0,3,4\}$, $\{0,2,8\}$, $\{0,5,10\}$. In this case,there is no value of d for which $L_S \bowtie L_T^d$.

We have extended the above calculations to all cyclic STS(v) for $v = 19, 21, 25, 27, 31$ and 33, using the orbit starters as listed in [1]. There are biembeddings of the Latin squares of the composition tables of the Steiner quasigroups obtained from all of these except for one cyclic STS(19), one cyclic STS(21), one cyclic STS(31), and one cyclic STS(33). In Table 1 we assume that the cyclic systems are in the same order as given in [1] with the system S being obtained from the orbit starters as listed there. The smallest value of d such that $L_S \bowtie L_T^d$ is given.

v	d
19	4, 8, 1, none
21	1, 6, 5, none, 2, 1, 3
25	2, 2, 1, 2, 1, 3, 7, 3, 2, 4, 4, 4
27	3, 10, 6, 1, 1, 2, 7, 2
31	1, 4, 4, 2, 15, 1, 1, 1, 4, 4, 4, 8, 4, 2, 1, 1, 8, 1, 1, 1, 9, 3, 2, 4, 2, 4, 2, 3, 2, 3, 4, 2, 4, 8, 2, 10, 1, 1, 1, 1, 1, 3, 1, 6, 3, 6, 4, 5, 1, 2, 5, 2, 1, 2, 1, 1, 2, 3, 1, 1, 2, 3, 1, 3, 5, 4, 8, 6, 4, 17, 1, 2, 4, none, 4, 2, 2, 1, 2, 1
33	3, 2, 1, 3, 1, 9, 1, 6, 4, 3, 3, 3, 1, 1, 1, 4, 1, 1, 16, 4, 6, 8, 3, 1, 3, 3, 1, 1, 1, 14, 2, 1, 1, 1, 2, 3, 1, 1, 2, 3, 1, 1, 1, 1, 1, 1, 1, 1, 2, 5, 2, 2, 1, 2, 1, 1, 2, 4, 1, 1, 1, 3, 3, 9, 1, 2, 4, 5, 1, 3, 1, 4, 3, 2, 3, 3, 8, 3, 3, 6, 1, 4, 1, none

Table 1: Self-embeddings of cyclic Steiner quasigroups.

We now prove that it is always possible to construct a biembedding from a solution to $\mathrm{HDP}_1(m)$ or $\mathrm{HDP}_2(m)$. We let L_S denote the Latin square of the composition table of the Steiner quasigroup obtained from the Steiner triple system S of order $v = 6m+1$ or $6m+3$, as appropriate. Assuming that the symbols of L_S use the standard labels $\{0, 1, \ldots, v-1\}$, we define L_S^d to be the Latin square obtained by adding $d \pmod{v}$ to every entry of the square L_S.

Theorem 2.3 *Let* $m \geq 1$*, let* $d \geq 1$ *satisfy* $\gcd(6m+1, d) = 1$*, and suppose that* $\bigcup_{i=1}^{m}\{\alpha_i, \beta_i, \gamma_i\}$ *is a solution to HDP*$_1(m)$*. Then there exists at least one pair* S, T *of cyclic STS*$(6m+1)$*s with orbit starters* $\{0, a_i, a_i+b_i\}$ *and* $\{0, b_i, a_i+b_i\}$ *respectively, where* $\{a_i, b_i\} = \{\alpha_i, \beta_i\}$*,* $1 \leq i \leq m$*, such that* $L_S \bowtie L_T^d$*.*

Proof. The proof is by iterative construction. By Theorem 2.1, it is sufficient to choose $a_i \in \{\alpha_i, \beta_i\}$, for $1 \leq i \leq m$, such that the rotation about the point 0_r consists of a single cycle (note that b_i is implied by the choice of a_i). Recall that the permutation obtained from the column entries of the rotations about the point 0_r is $P_2 R^{-d} P_1$, where the involutions P_1 and P_2 are defined as in the proof of Theorem 2.1. This permutation is conjugate to $P_2 P_1 R^d$, so the problem is reduced to selecting a_i, for $1 \leq i \leq m$, such that $P_2P_1R^d$ consists of a single permutation cycle. From the definitions of P_1 and P_2 we have

$$P_2P_1R^d = \left(\prod_{1 \leq i \leq m} (\ a_i\ \ b_i\ \ (-a_i - b_i)\ )(-b_i\ \ \ -a_i\ \ (a_i + b_i)\ ) \right) R^d.$$

In order to proceed iteratively, we define

$$Q_k = \left(\prod_{1 \leq i \leq k} (\ a_i\ \ b_i\ \ (-a_i - b_i)\ )(-b_i\ \ \ -a_i\ \ (a_i + b_i)\ ) \right) R^d,$$

for $0 \leq k \leq m$. We say that a Q_k is *adequate* if it consists of a single permutation cycle, and has the additional property that $Q_k^t(0) = -Q_k^{-t}(0)$ for any t provided that $Q_k^t(0) \notin \bigcup_{1 \leq i \leq k}\{a_i, -a_i, b_i, -b_i, a_i + b_i, -a_i - b_i\}$. Since $\gcd(d, 6m+1) = 1$, the permutation $Q_0 = R^d$ is adequate. We select each a_k in turn, $k = 1, 2, \ldots m$, in such a way that Q_k is adequate. This is possible provided that, for each $k \in \{1, 2, \ldots, m\}$, and assuming that Q_{k-1} is adequate, one of the two following choices of Q_k is adequate:

$$\begin{aligned}
&(\ \alpha_k\ \ \beta_k\ \ (-\alpha_k - \beta_k)\ )(-\beta_k\ \ \ -\alpha_k\ \ (\alpha_k + \beta_k)\ )Q_{k-1},\\
&(\ \beta_k\ \ \alpha_k\ \ (-\alpha_k - \beta_k)\ )(-\alpha_k\ \ \ -\beta_k\ \ (\alpha_k + \beta_k)\ )Q_{k-1}.
\end{aligned}$$

Note that $\alpha_k, \beta_k, \alpha_k+\beta_k, -\alpha_k, -\beta_k, -\alpha_k-\beta_k$ are distinct elements of $\{1, 2, \ldots, 6m\} \backslash \bigcup_{1 \leq i \leq k-1}\{a_i, -a_i, b_i, -b_i, a_i+b_i, -a_i-b_i\}$, from the definition of $\mathrm{HDP}_1(m)$. Define $x_i = Q_{k-1}^i(0)$, so $Q_{k-1} = (0\ x_1\ x_2\ \ldots\ x_{6m})$. Then for some $A, B, C \in \{1, 2, \ldots, 6m\}$ we have $\alpha_k = x_A$, $\beta_k = x_B$, and $-\alpha_k - \beta_k = x_C$. By assumption Q_{k-1} is adequate, so $-\alpha_k = x_{-A}$, $-\beta_k = x_{-B}$, and $\alpha_k + \beta_k = x_{-C}$. Thus Q_k is equal to either

$$(x_A\ x_B\ x_C)(x_{-B}\ x_{-A}\ x_{-C})Q_{k-1},\ \text{or}$$

$$(x_B\ x_A\ x_C)(x_{-A}\ x_{-B}\ x_{-C})Q_{k-1},$$

where $A, B, C, -A, -B, -C$ are all distinct. This remains true after any permutation of the labels A, B, C, or after swapping the labels A, B and C with $-A$, $-B$ and $-C$ respectively (note that in each case, the actions of the two three-cycles are independent and so their order is irrelevant); therefore we may assume without loss of generality that $1 \leq A < B < \min\{C, 3m+1\}$. We now break the problem into four cases based on the size of C relative to

$v-A$, $v-B$ and $v-C$, where $v=6m+1$. In each case we write down the permutation Q_{k-1} and one of the two possibilities for Q_k. They are written in permutation cycle notation with terms of the form S_i used to represent partial permutation cycles $\ldots x_p\, x_{p+1} \ldots x_{q-1}\, x_q \ldots$, where $q \geq p$.

Case 1: $1 \leq A < B < C < v-C < v-B < v-A \leq v-1$;

$$\begin{aligned} Q_{k-1} &= (0\ S_1\ x_A\ S_2\ x_B\ S_3\ x_C\ S_4\ x_{-C}\ S_5\ x_{-B}\ S_6\ x_{-A}\ S_7), \\ Q_k &= (x_A\ x_B\ x_C)(x_{-B}\ x_{-A}\ x_{-C})Q_{k-1} \\ &= (0\ S_1\ x_B\ S_3\ x_A\ S_2\ x_C\ S_4\ x_{-B}\ S_6\ x_{-C}\ S_5\ x_{-A}\ S_7). \end{aligned}$$

Case 2: $1 \leq A < B < v-C < C < v-B < v-A \leq v-1$;

$$\begin{aligned} Q_{k-1} &= (0\ S_1\ x_A\ S_2\ x_B\ S_3\ x_{-C}\ S_4\ x_C\ S_5\ x_{-B}\ S_6\ x_{-A}\ S_7), \\ Q_k &= (x_A\ x_B\ x_C)(x_{-B}\ x_{-A}\ x_{-C})Q_{k-1} \\ &= (0\ S_1\ x_B\ S_3\ x_{-B}\ S_6\ x_{-C}\ S_4\ x_A\ S_2\ x_C\ S_5\ x_{-A}\ S_7). \end{aligned}$$

Case 3: $1 \leq A < v-C < B < v-B < C < v-A \leq v-1$;

$$\begin{aligned} Q_{k-1} &= (0\ S_1\ x_A\ S_2\ x_{-C}\ S_3\ x_B\ S_4\ x_{-B}\ S_5\ x_C\ S_6\ x_{-A}\ S_7), \\ Q_k &= (x_B\ x_A\ x_C)(x_{-A}\ x_{-B}\ x_{-C})Q_{k-1} \\ &= (0\ S_1\ x_C\ S_6\ x_{-B}\ S_5\ x_B\ S_4\ x_{-C}\ S_3\ x_A\ S_2\ x_{-A}\ S_7). \end{aligned}$$

Case 4: $1 \leq v-C < A < B < v-B < v-A < C \leq v-1$;

$$\begin{aligned} Q_{k-1} &= (0\ S_1\ x_{-C}\ S_2\ x_A\ S_3\ x_B\ S_4\ x_{-B}\ S_5\ x_{-A}\ S_6\ x_C\ S_7), \\ Q_k &= (x_A\ x_B\ x_C)(x_{-B}\ x_{-A}\ x_{-C})Q_{k-1} \\ &= (0\ S_1\ x_{-B}\ S_5\ x_{-C}\ S_2\ x_B\ S_4\ x_{-A}\ S_6\ x_A\ S_3\ x_C\ S_7). \end{aligned}$$

In each case we can choose $a_k \in \{\alpha_k, \beta_k\}$ so that Q_k is as given, and hence consists of a single permutation cycle. Furthermore, from the assumption that Q_{k-1} is adequate and the observation that S_i has the same length as S_{8-i}, for $i = 1, 2, 3$, and that the symmetry between S_i and S_{8-i} is preserved in Q_k, we see that in each case Q_k is adequate. Proceeding iteratively, we obtain a choice of $a_1, a_2, \ldots, a_m$ such that $Q_m = P_2 P_1 R^d$ is adequate. $\square$

This construction can be readily extended to cyclic STS$(6m+3)$s based on a solution to HDP$_2(m)$, and a difference d satisfying $\gcd(d, 6m+3) = 1$.

The construction is the same, except that $v = 6m+3$ and

$$P_1 = \prod_{1\le i\le m} (a_i \ \ (a_i+b_i))(-a_i \ \ b_i)((-a_i-b_i) \ \ -b_i)((2m+1) \ \ (4m+2)),$$

$$P_2 = \prod_{1\le i\le m} (a_i \ \ -b_i)((a_i+b_i) \ \ b_i)(-a_i \ \ (-a_i-b_i))((2m+1) \ \ (4m+2)).$$

The permutation P_2P_1 is unchanged, except that there are three fixed points, namely 0, $2m+1$ and $4m+2$, rather than just one (0). Thus we have the following theorem:

Theorem 2.4 *Let* $m \ge 1$, *let* $d \ge 1$ *satisfy* $\gcd(6m+3, d) = 1$, *and suppose that* $\bigcup_{i=1}^{m}\{\alpha_i, \beta_i, \gamma_i\}$ *is a solution to* $HDP_2(m)$. *Then there exists at least one pair* S, T *of cyclic* $STS(6m+3)s$ *with full orbit starters* $\{0, a_i, a_i+b_i\}$ *and* $\{0, b_i, a_i+b_i\}$ *respectively, where* $\{a_i, b_i\} = \{\alpha_i, \beta_i\}$, $1 \le i \le m$, *together with the short orbit starter* $\{0, 2m+1, 4m+2\}$ *in each case, such that* $L_S \bowtie L_T^d$.

Note that this construction does not explicitly define a_i, for $1 \le i \le m$, but only states that a_i may be selected from $\{\alpha_i, \beta_i\}$, $1 \le i \le m$, in such a way that $L_S \bowtie L_T^d$. Computationally, S and T may be readily obtained from a given solution to $\mathrm{HDP}_1(m)$ or $\mathrm{HDP}_2(m)$ by following the iterative method given in the proof. Note also that the Latin squares L_S and L_T^d will always be paratopic.

3 Self-embeddings of the projective Steiner quasigroups.

Throughout this section we suppose that $n \ge 2$ and take $m = 2^n$. The projective Steiner triple system of order $m-1$ is the point-line design of the projective geometry $\mathrm{PG}(n-1, 2)$ and may be written as

$$\{\{a, b, c\} \mid a, b, c \text{ distinct elements of } \mathrm{GF}(m) \setminus \{0\},\ a+b+c = 0\}.$$

This is a cyclic Steiner triple system since, for any primitive element x of $\mathrm{GF}(m) \setminus \{0\}$, we have $x^i + x^j + x^k = 0$ if and only if $x^{i+r} + x^{j+r} + x^{k+r} = 0$. We will biembed the corresponding Steiner quasigroup with a paratopic copy of itself using a construction equivalent to that used in Section 2 (we may take the discrete logarithm to base x to make this equivalence explicit). Although projective Steiner triple systems only exist for orders $2^n - 1$, this construction is explicit, unlike the iterative construction for Theorems 2.3 and 2.4; furthermore, we show that the set of permissible values of d may be obtained from the set of monic second degree primitive polynomials over GF(m). We begin with two preliminary lemmas.

Lemma 3.1 *Suppose that $p(z) = z^2 + az + b$ is a primitive polynomial over GF(m). Take $c \in$ GF(m) such that $b = c^2$, and put $\alpha = a/c$. Then the polynomial $q(w) = w^2 + \alpha w + 1$ is irreducible over GF(m) and if $\omega \in$ GF(m^2) is a root of q, then ω has order $m + 1$. Furthermore, c has order $m - 1$.*

Proof. Since q is obtained from p by the linear transformation $w = z/c$, it is trivial that q is irreducible over GF(m). Suppose that $\omega = \zeta/c \in \mathrm{GF}(m^2)$ is a root of q, so that ζ is a root of p. If ω has order r, then r is the smallest positive integer for which $\zeta^r = c^r$. But then $\zeta^{r(m-1)} = c^{r(m-1)} = 1$ since $c \in \mathrm{GF}(m)$. However, ζ has order $m^2 - 1 = (m - 1)(m + 1)$. It follows that r must be a positive integer multiple of $m + 1$. It is also the case that $\alpha = \omega + 1/\omega$, and so $\alpha^m = \omega^m + 1/\omega^m$. But $\alpha \in \mathrm{GF}(m)$, so that $\alpha^m = \alpha$, and this gives $\omega + 1/\omega = \omega^m + 1/\omega^m$. Consequently $(\omega^{m-1} + 1)(\omega^{m+1} + 1) = 0$, and since $\omega^{m-1} \neq 1$ it follows that $\omega^{m+1} = 1$. Therefore r is also a factor of $m + 1$. Hence $r = m + 1$, that is to say ω has order $m + 1$. Furthermore $\zeta^{m+1} = c^{m+1} = c^2 = b$. Since ζ^{m+1} has order $m - 1$, it follows that b and hence c have order $m - 1$. □

Lemma 3.2 *Suppose that $\alpha \in$ GF(m) and that $q(w) = w^2 + \alpha w + 1$ has a root ω of order $m + 1$ in GF(m^2). Take any $c \in$ GF(m) having order $m - 1$ and put $a = \alpha c$ and $b = c^2$. Then $p(z) = z^2 + az + b$ is a primitive polynomial over GF(m).*

Proof. Because the order of ω in GF(m^2) is $m + 1$, $\omega \notin \mathrm{GF}(m)$, and so q is irreducible over GF(m). Since p is obtained from q by the linear transformation $z = cw$, it is trivial that p is irreducible over GF(m) and that $\zeta = c\omega \in \mathrm{GF}(m^2)$ is a root of p. Suppose that ζ has order r. Then $c^r\omega^r = 1$ and so $c^{r(m+1)}\omega^{r(m+1)} = 1$. Hence $c^{r(m+1)} = 1$ and consequently $c^{2r} = 1$ and thus $c^r = 1$. Since $c \in \mathrm{GF}(m)$ has order $m - 1$, r must be a positive integer multiple of $m - 1$. But then $c^r\omega^r = 1$ gives $\omega^r = 1$, so that r is also a positive integer multiple of $m + 1$. Since r cannot be larger than $m^2 - 1 = (m - 1)(m + 1)$, it follows that $r = m^2 - 1$. Hence p is a primitive polynomial over GF(m). □

Theorem 3.1 *For $n \geq 2$, the projective Steiner quasigroup of order $2^n - 1$ has a biembedding with a paratopic copy of itself.*

Proof. Suppose that x is a primitive element of $\mathrm{GF}(m)$. Let L_S denote the Cayley table of the projective Steiner quasigroup of order $m-1$ with row labels, column labels and entries from $\mathrm{GF}(m)\backslash\{0\}$ such that $(x^i, x^j, x^k) \in L_S$, that is $x^k = L_S(x^i, x^j)$, where i, j, k are integers satisfying $0 \leq i, j, k \leq m-2$, if and only if either (a) $i \neq j$ and $x^i + x^j + x^k = 0$, or (b) $i = j = k$.

Define L_T to be the Latin square formed from L_S by applying the mapping $x^i \to x^{m-1-i}$, $0 \leq i \leq m-2$, to the row labels, the column labels and the entries of L_S, and for each integer d satisfying $0 \leq d \leq m-2$, define L_T^d to be the Latin square formed from L_T by applying the mapping $x^i \to x^{i+d}$, $0 \leq i \leq m-2$, to the entries. Thus, for $0 \leq i, j, k \leq m-2$ we have $(x^i, x^j, x^k) \in L_T^d$ if and only if either (a) $i \neq j$ and $x^k = x^{i+j+d}/(x^i + x^j)$, or (b) $i = j = k - d$. Clearly L_T^d is paratopic to L_S. We will prove that, for suitable choices of d, $L_S \bowtie L_T^d$.

For a given x, we can apply the mapping $x^i \mapsto i$ to the row, column and symbol labels of L_S, L_T and L_T^d to obtain Latin squares L_S^*, L_T^* and L_T^{d*} with the standard row, column and entry labels $\{0, 1, \ldots, m-2\}$. Then L_S^* and L_T^* are the Steiner quasigroups corresponding to the Steiner triple systems cyclically generated from the orbit starters $\{\{0, a, a+b\} \mid 1 + x^a + x^{a+b} = 0\}$ and $\{\{0, b, a+b\} \mid 1 + x^b + x^{a+b} = 0\}$, respectively, and L_T^{d*} is obtained from L_T^* by adding d (mod $m-1$) to every entry. By Theorems 2.1 and 2.2, $L_S^* \bowtie L_T^{d*}$ if and only if the rotation about row 0 is a complete cycle; equivalently $L_S \bowtie L_T^d$ if and only if the rotation about row $1 = x^0$ is a complete cycle. Thus we proceed by examining the rotation about row 1.

The rotation at row vertex $1 = x^0$ alternates column and entry vertices. Note that the entry x^k appears in row 1 of L_T^d in the column x^j given by

$$x^j = \begin{cases} x^k/(x^d + x^k) & \text{if } \ k \neq d, \\ 1 & \text{if } \ k = d. \end{cases}$$

Starting with the column vertex $1 + x^d$ appearing in L_S, the alternating sequence of column and entry vertices in the rotation at 1 is given by

$$\begin{array}{cccccccccc} \text{col.} & \text{entry} & \text{col.} & \text{entry} & \text{col.} & \cdots & \text{col.} & \text{entry} & \text{col.} & \cdots \\ 1+x^d & x^d & 1 & 1 & \frac{1}{(1+x^d)} & \cdots & z & z+1 & \frac{z+1}{z+1+x^d} & \cdots \end{array}$$

Denote the sequence of column vertices, starting from column 1, by $\kappa_0, \kappa_1, \kappa_2, \ldots$, and set $\alpha = x^d$. Then $\kappa_0 = 1, \kappa_1 = 1/(1+\alpha)$ and $\kappa_{r+1} =$

$(\kappa_r + 1)/(\kappa_r + 1 + \alpha)$ for $r \geq 1$ until $\kappa_r = 1 + \alpha$ and then $\kappa_{r+1} = 1 = \kappa_0$. In order for the rotation at row vertex 1 to be a single cycle of length $2m-2$ it is therefore necessary and sufficient that the set of values $\{\kappa_0, \kappa_1, \ldots, \kappa_{m-2}\} = \mathrm{GF}(m) \setminus \{0\}$. (As an aside, note that the map $\kappa_i \mapsto \kappa_{i+1}$ is equivalent to the action of the permutation $P_2 R^{-d} P_1$ in the proof of Theorem 2.1.)

Now consider the mapping $f : z \to (z+1)/(z+1+\alpha)$ on $\mathrm{GF}(m) \cup \{\infty\}$. Put $z_0 = \infty$ and $z_{r+1} = f(z_r)$ for $r \geq 0$. Then the first few terms of the sequence (z_r) are $\infty, 1, 0, 1/(1+\alpha), \ldots$. Comparing this with (κ_r), we have $\kappa_0 = z_1, \kappa_1 = z_3$ and $\kappa_r = z_{r+2}$ for $r \geq 1$ until $\kappa_r = z_{r+2} = 1 + \alpha$ and thus $z_{r+3} = z_0 = \infty$ and $\kappa_{r+1} = \kappa_0 = 1$. So proving that $\{\kappa_0, \kappa_1, \ldots, \kappa_{m-2}\} = \mathrm{GF}(m) \setminus \{0\}$ is equivalent to proving that $\{z_0, z_1, \ldots, z_m\} = \mathrm{GF}(m) \cup \{\infty\}$.

Next define sequences (a_r) and (b_r) in $\mathrm{GF}(m)$ by $(a_0, b_0) = (1, 0)$ and $(a_{r+1}, b_{r+1}) = (\alpha b_r, a_r + \alpha b_r)$ for $r \geq 0$. Inductively, $z_r = (a_r + b_r)/b_r$ for $r \geq 0$. Note that $a_{r+2} = \alpha b_{r+1} = \alpha a_r + \alpha^2 b_r = \alpha a_r + \alpha a_{r+1}$. So (a_r) satisfies the second order recurrence relationship $a_{r+2} + \alpha a_{r+1} + \alpha a_r = 0$.

To obtain a closed expression for a_r, consider the auxiliary equation $\theta^2 + \alpha\theta + \alpha = 0$. This may or may not have roots in $\mathrm{GF}(m)$ depending on whether the equation is reducible or irreducible over $\mathrm{GF}(m)$. In the irreducible case, we may assume that it has roots in $\mathrm{GF}(m^2)$, and in either case we will denote the roots as θ_1 and $\theta_1 + \alpha$. Note that $\theta_1 \neq 0, 1, \alpha, 1 + \alpha$. The recurrence relationship has solution

$$a_r = C\theta_1^r + D(\theta_1 + \alpha)^r$$

for some constants C and D. However, $a_0 = 1$ and $a_1 = 0$ and these give $C = (\theta_1 + \alpha)/\alpha$ and $D = \theta_1/\alpha$ so that

$$a_r = \theta_1(\theta_1 + \alpha)[\theta_1^{r-1} + (\theta_1 + \alpha)^{r-1}]/\alpha.$$

But $b_r = a_{r+1}/\alpha$, so

$$b_r = \theta_1(\theta_1 + \alpha)[\theta_1^r + (\theta_1 + \alpha)^r]/\alpha^2.$$

Clearly, the lowest value of $r > 0$ for which $z_r = (a_r + b_r)/b_r = \infty$ is given by the lowest value of $r > 0$ for which $\theta_1^r + (\theta_1 + \alpha)^r = 0$, that is to say $(1 + \alpha/\theta_1)^r = 1$. At this point we observe that if $\theta_1 \in \mathrm{GF}(m)$ then $(1 + \alpha/\theta_1)^{m-1} = 1$ and so $z_{m-1} = \infty$. We therefore require $\theta_1 \notin \mathrm{GF}(m)$, so that $\theta^2 + \alpha\theta + \alpha$ must be irreducible over $\mathrm{GF}(m)$.

Since $\theta_1^2 + \alpha\theta_1 + \alpha = 0$, then $1 + \alpha/\theta_1 = 1/(\theta_1 + 1)$, so $(1 + \alpha/\theta_1)^r = 1$ if and only if $(\theta_1 + 1)^r = 1$. Defining $\phi_1 = \theta_1 + 1 \in \mathrm{GF}(m^2)$, we have established that $L_S \bowtie L_T^d$ if and only if ϕ_1 has order $m+1$. Now ϕ_1 is a root of the irreducible polynomial $\phi^2 + \alpha\phi + 1 = 0$ over $\mathrm{GF}(m)$, where $\alpha = x^d$. By applying Lemmas 3.1 and 3.2, all permissible values of α for which $L_S \bowtie L_T^d$ are obtained by taking each monic second degree primitive polynomial over $\mathrm{GF}(m)$, say $z^2 + az + c^2$, and setting $\alpha = a/c$. Since such polynomials exist for all $n \geq 2$, the theorem is proven. $\square$

4 Concluding remarks

We turn briefly to lower bounds on the numbers of biembeddings. In [12] it was proved that for $n = 3p$, where $p = 3(2^{2t+1} - 1)$ and t is sufficiently large, there are at least $n^{\frac{n^2}{144}(1-o(1))}$ nonisomorphic face 2-colourable triangular embeddings of $K_{n,n,n}$, each of which has a parallel class in one colour. The proof depends on the construction of a biembedding of a pair of Latin squares of side p, one of which has $p(p-3)(p-9)/12$ subsquares of side 2, and the other has a transversal. However, Theorem 3.1 establishes that for $t \geq 2$, there is a biembedding of a pair of Latin squares of side $q = 2^t - 1$, each of which has $q(q-1)(q-3)/4$ subsquares of side 2 and a transversal. By using this biembedding and employing the same arguments as in [7, 12], the result is easily extended to values of n of the form $n = 3q$, where $q = 2^t - 1$: if t is sufficiently large then there are at least $n^{\frac{n^2}{144}(1-o(1))}$ nonisomorphic face 2-colourable triangular embeddings of $K_{n,n,n}$, each of which has a parallel class in one colour. Using this estimate, it is possible to extend the lower bounds given in [7, 12] for the numbers of nonisomorphic face 2-colourable triangular embeddings of K_r in both orientable and nonorientable surfaces to a wider range of values of r. As a specific example, by combining these embeddings of $K_{n,n,n}$ with the face 2-colourable triangular embedding of K_7 and using construction 5 from [10], we obtain at least $r^{\frac{r^2}{1296}(1-o(1))}$ nonisomorphic face 2-colourable triangular embeddings of K_r in an orientable surface for values of r of the form $r = 6n + 1 = 18(2^t - 1) + 1$.

Acknowledgements The second and third authors thank the University of Queensland and their co-authors for their hospitality.

References

[1] M. J. Colbourn and R. A. Mathon, *On cyclic Steiner* 2*-designs*, in "Topics on Steiner systems", Ann. Discrete Math. **7** (1980), 215–253.

[2] C. J. Colbourn and A. Rosa, *Triple systems*, Oxford University Press, New York (1999).

[3] D. M. Donovan, A. Drápal, M. J. Grannell, T. S. Griggs and J. G. Lefevre, *Quarter-regular biembeddings of Latin squares*, Discrete Math. **310** (2010), 692–699.

[4] D. M. Donovan, M. J. Grannell and T. S. Griggs, *Third-regular biembeddings of Latin squares*, Glasgow Math. J., to appear.

[5] L. Heffter, *Űber Tripelsysteme*, Math. Ann. **49** (1897), 101–112.

[6] M. J. Grannell and T. S. Griggs, *Designs and topology* in "Surveys in Combinatorics 2007", 121–174, London Math. Soc. Lecture Note Ser., 346, Cambridge Univ. Press, Cambridge, 2007.

[7] M. J. Grannell and T. S. Griggs, *A lower bound for the number of triangular embeddings of some complete graphs and complete regular tripartite graphs*, J. Combin. Theory Ser. B **98** (2008), 637–650.

[8] M. J. Grannell, T. S. Griggs and M. Knor, *Biembeddings of Latin squares and Hamiltonian decompositions*, Glasgow Math. J. **46** (2004), 443–457.

[9] M. J. Grannell, T. S. Griggs and M. Knor, *On biembeddings of Latin squares*, Electron. J. Combin. **16** (2009), R106, 12pp.

[10] M. J. Grannell, T. S. Griggs and J. Širáň, *Recursive constructions for triangulations*, J. Graph Theory **39** (2002), 87–107.

[11] M. J. Grannell and M. Knor, *Biembeddings of Abelian groups*, J. Combin. Des. **18** (2010), 71–83.

[12] M. J. Grannell and M. Knor, *A lower bound for the number of orientable triangular embeddings of some complete graphs*, J. Combin. Theory Ser. B, to appear.

[13] J. L. Gross and T. W. Tucker, *Topological Graph Theory*, John Wiley, New York (1987).

[14] T. P. Kirkman, *On a problem in combinations*, Cambridge and Dublin Math. J. **2** (1847), 191–204.

[15] R. Peltesohn, *Eine Lösung der beiden Heffterschen Differenzenprobleme*, Compositio Math. **6** (1939), 251–257.

[16] G. Ringel, *Map color theorem*, Springer-Verlag, New York and Berlin (1974).

[17] S. Stahl and A. T. White, *Genus embeddings for some complete tripartite graphs*, Discrete Math. **14** (1976), 279–296.